La cyber-security in azienda

Vulnerabilità, modelli di prevenzione, strumenti e strategie di gestione del rischio

Paradigma presso Hotel Hilton, 28 settembre 2017

DEEPCYBER

Advanced Intelligence, Protection, Antifraud.

Gerardo Costabile
gerardo.costabile@deepcyber.it

3 steps today

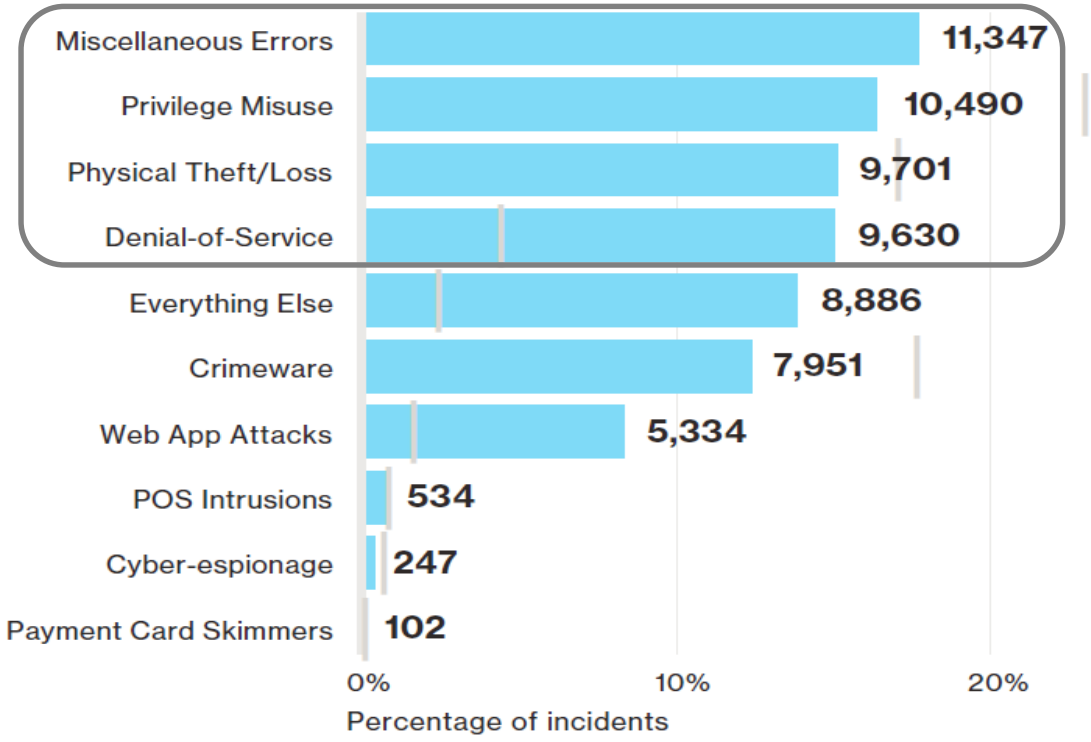
1. Analisi nuove minacce e lesson learned

2. Architettura di cyber security in IoT, ICS, etc

3. Cyber threat intelligence maturity model

DEEPCYBER

Le principali cause di *data breaches* sono riconducibili a problematiche non riscontrabili in assessment process based



Fonte DBIR

Lessons Learned

Gli assessment condotti in modalità tradizionale process based non permettono di misurare efficacemente i rischi riconducibili alle cause della maggioranza dei data breach rilevati (errori umani, abuso dei privilegi di accesso, furti di tipo fisico e attacchi DOS)

DEEPCYBER

Anche gli ATM sono oggetto di attacchi sempre più evoluti mediante l'utilizzo di virus informatici

- Il criminale informatico «attiva» abusivamente l'ATM con l'inserimento di una carta che contiene alcuni record specifici sulla banda magnetica.
- Dopo aver letto la carta, Skimer è in grado di eseguire o ricevere comandi attraverso un menù speciale attivato dalla carta.
- A schermo viene visualizzata una specifica interfaccia utente solo a seguito di specifici comandi nella sessione, entro i 60 secondi.
- Il menu offre 21 diverse opzioni, tra cui l'erogazione di denaro, la raccolta dei dettagli delle carte che sono state inserite nell'ATM, l'auto-cancellazione e l'esecuzione di aggiornamenti.

Attacco Ddos Iot – 21 ottobre 2016

LA STAMPA MONDO

SEGUICI SU ACCE

Un attacco hacker ha messo KO internet negli Stati Uniti

Centinaia di siti sono stati irraggiungibili per ore in seguito a un DDoS, tra cui Twitter, Spotify, Reddit, eBay e PayPal

La causa: il malware Mirai - creato per infettare dispositivi IoT (Internet di Things) ed è stato utilizzato come piattaforma per lanciare attacchi di tipo DDoS.

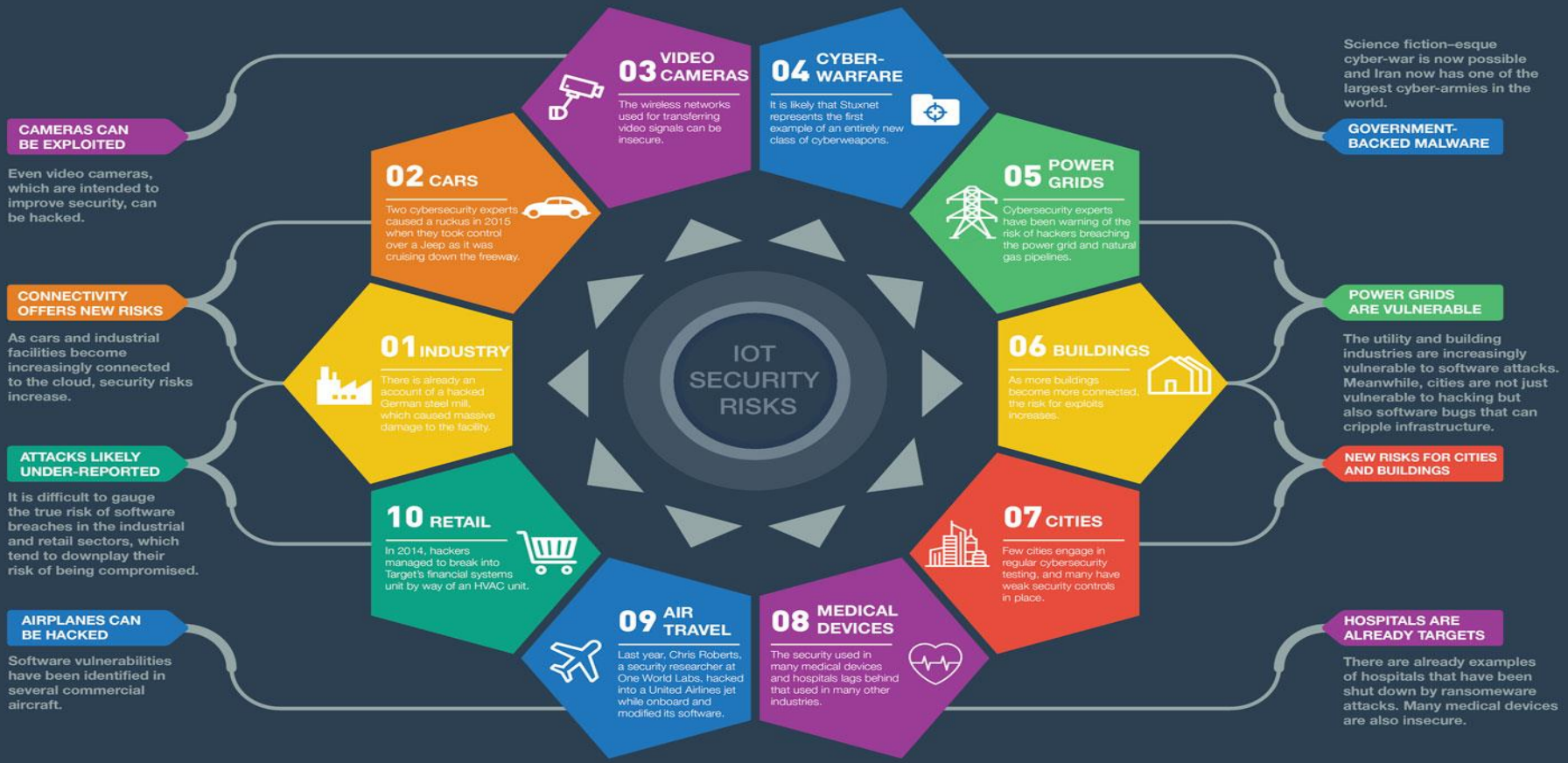
Mirai è costruito per due scopi principali:

1. Individuare (attraverso scansioni ad ampio raggio) e compromettere (attraverso l'accesso remoto) i dispositivi IoT e agganciarli alla botnet.
2. Lanciare attacchi DDoS basati su istruzioni ricevute dalla C&C.

Mirai utilizza una tecnica forza bruta per indovinare la password dei dispositivi e tecniche di flooding sui protocolli HTTP, GRE IP-GRE ETH, o con SYN-ACK flood e STOMP flooding.

10 IoT **Security** Targets

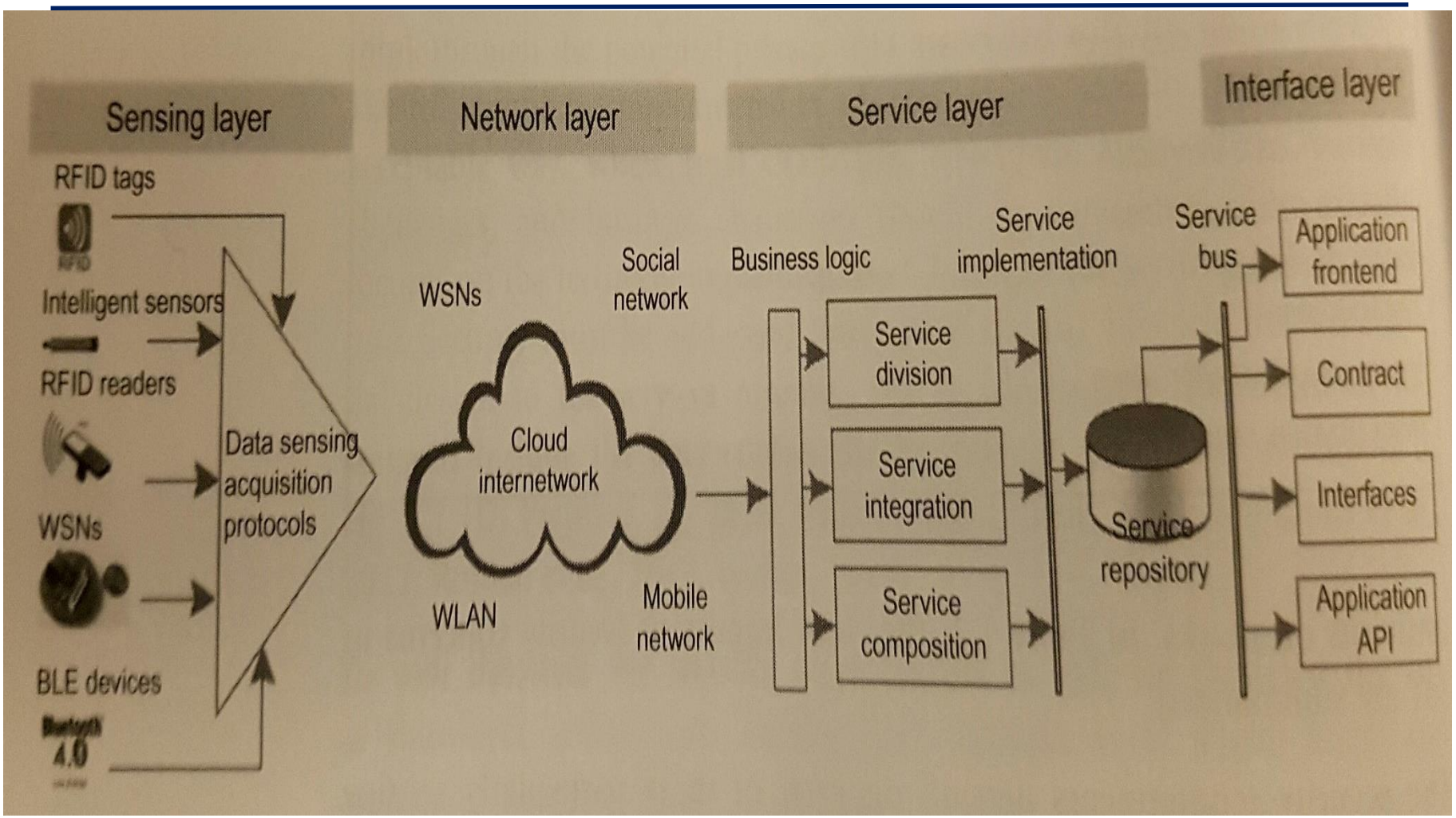
Internet of Things INSTITUTE



Penton
1166 Avenue of the Americas
10th Floor
New York, NY 10036
Phone: 212 204 4200
www.penton.com
www.ioti.com

Infographic templatae courtesy of iStock / thebackground

Architettura «tipica» dei servizi IoT

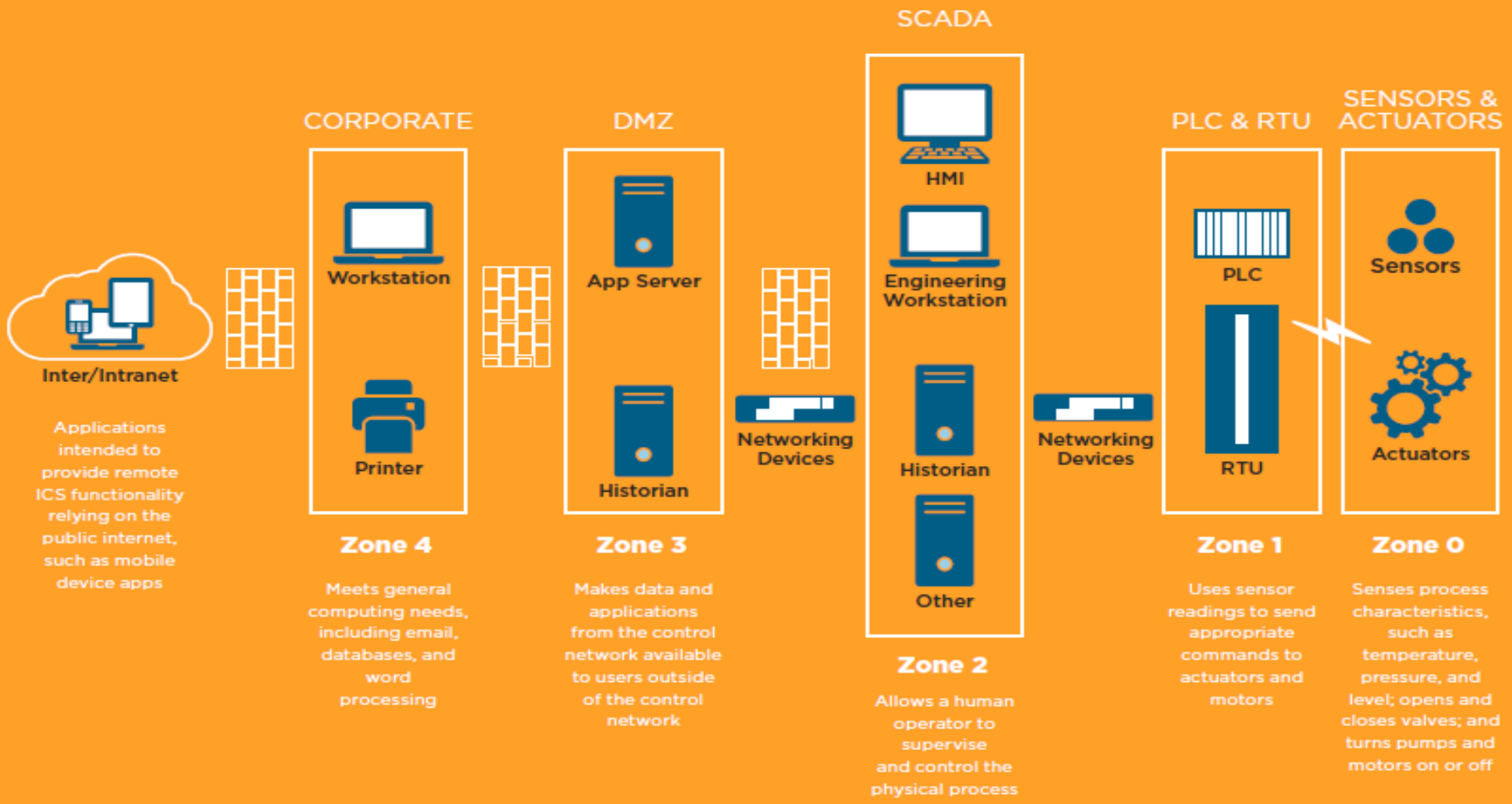


Source: Shancang Li/Li Da Xu – Securing the IoT - 2017

DEEPCYBER

Interconnectivity of computers - manufacturing systems

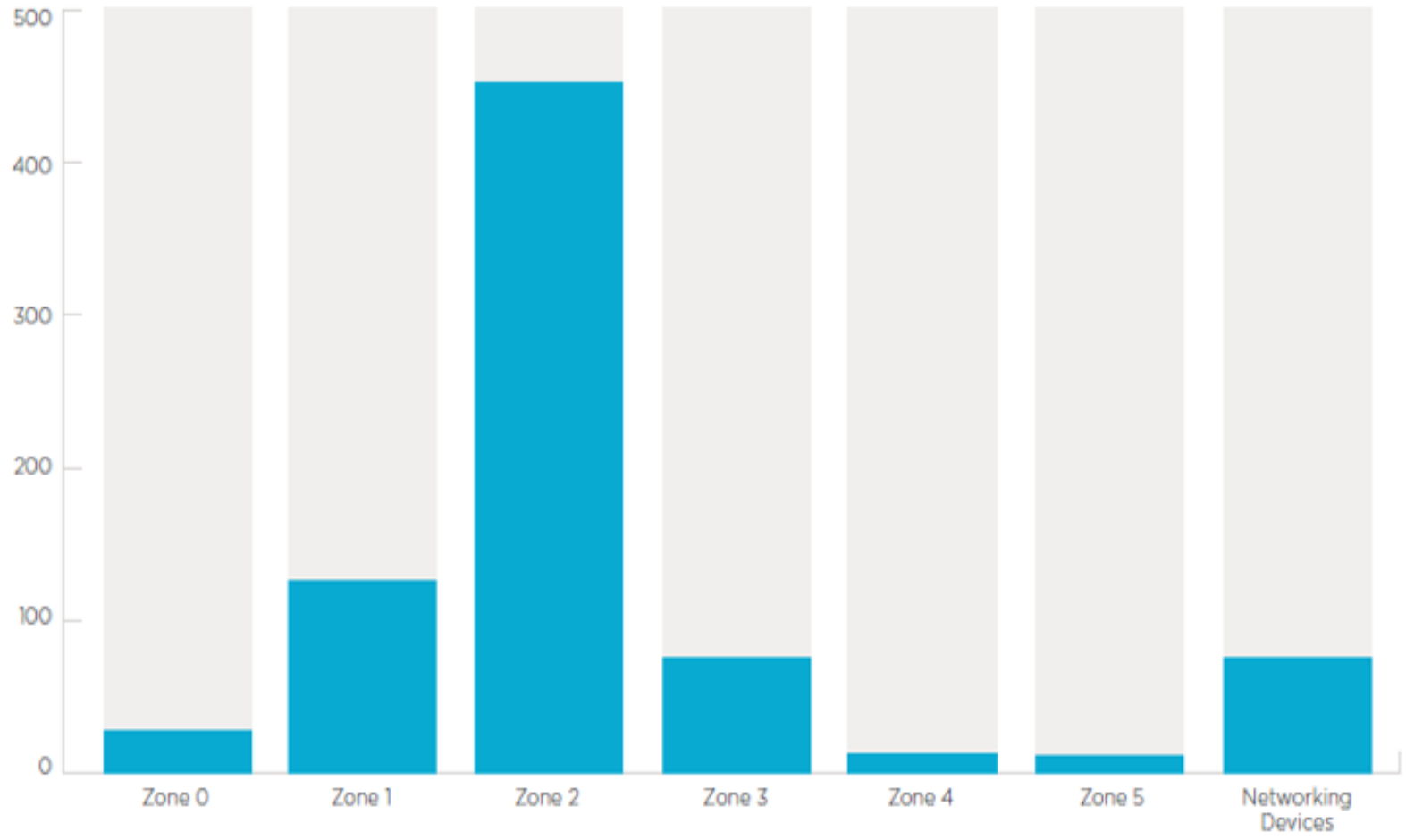
Source: 2016 Industrial Control Systems (ICS) Vulnerability Trend Report - FireEye



[4] The Simplified Purdue model refers to a framework developed by researchers to describe the interconnectivity of computers to manufacturing systems.

Specific vulnerability disclosures affecting each level

Source: 2016 Industrial Control Systems (ICS) Vulnerability Trend Report - FireEye

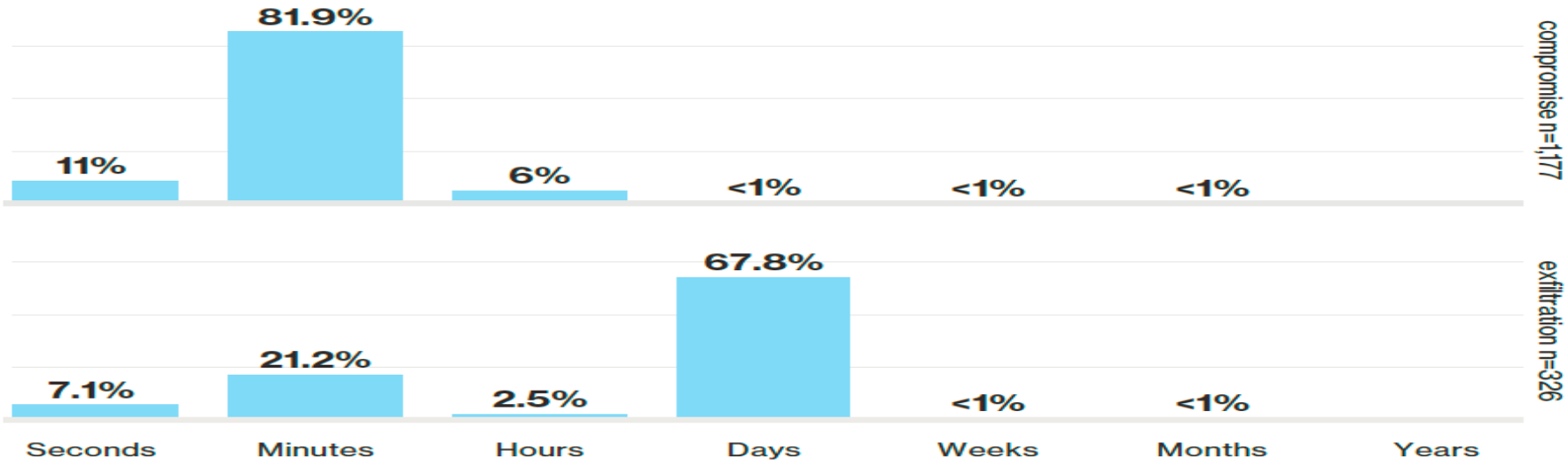


Incident patterns by industry
(source: DBIR)

Crimeware	Cyber-espionage	Denial of Service	Everything Else	Stolen Assets	Misc. Errors	Card Skimmers	Point of Sale	Privilege Misuse	Web Apps	Incident patterns by industry minimum 25 incidents
<1%	<1%	20%	1%	1%	1%	<1%	74%	2%	1%	Accommodation (72), n=362
		56%	4%		2%		4%	22%	11%	Administrative (56), n=44
2%	2%	81%	2%	3%	4%			1%	5%	Educational (61), n=254
		99%		<1%			1%		1%	Entertainment (71), n=2,707
2%	<1%	34%	5%	<1%	1%	6%	<1%	3%	48%	Finance (52), n=1,368
4%	2%		11%	32%	18%		5%	23%	4%	Healthcare (62), n=166
4%	3%	46%	21%	<1%	11%		<1%	2%	12%	Information (51)n, 1,028
5%	16%	33%	33%		1%		1%	6%	6%	Manufacturing (31-33), n=171
1%	2%	90%	2%	1%	1%			2%	1%	Professional (54), n=916
16%	<1%	1%	17%	20%	24%		<1%	22%	<1%	Public (92), n=47,237
1%	<1%	45%	2%		1%	3%	32%	1%	13%	Retail (44-45), n=370
10%	16%	26%			6%			6%	35%	Transportation (48-49), n=31

DEEPCYBER

Time to compromise vs time to discover
(source: DBIR)



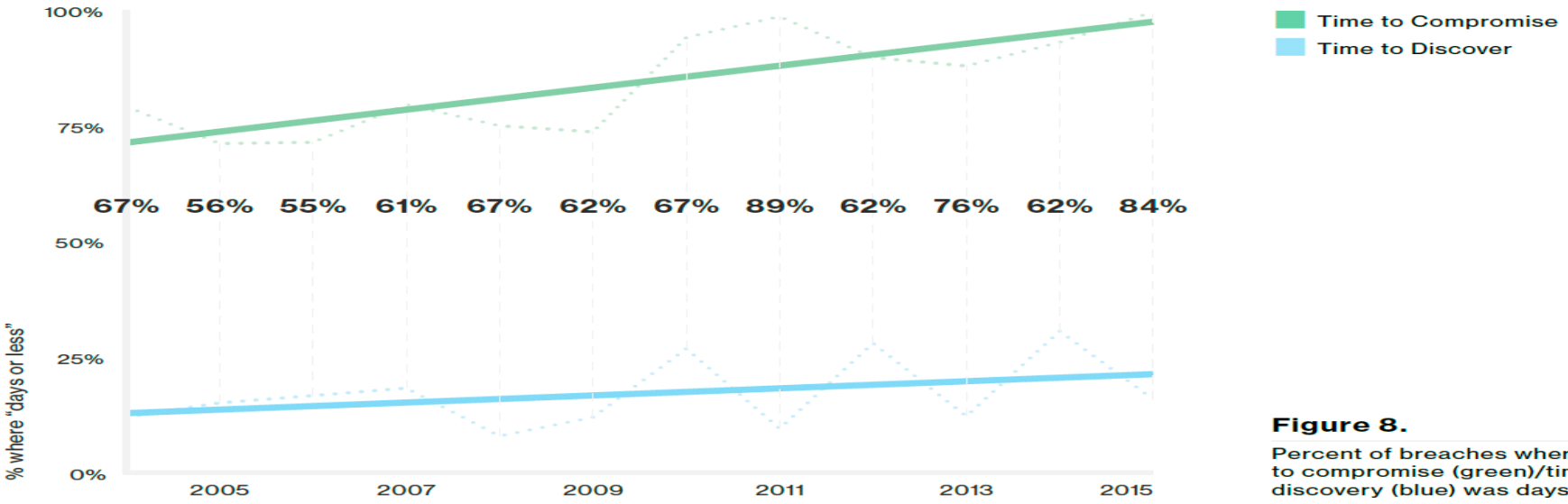
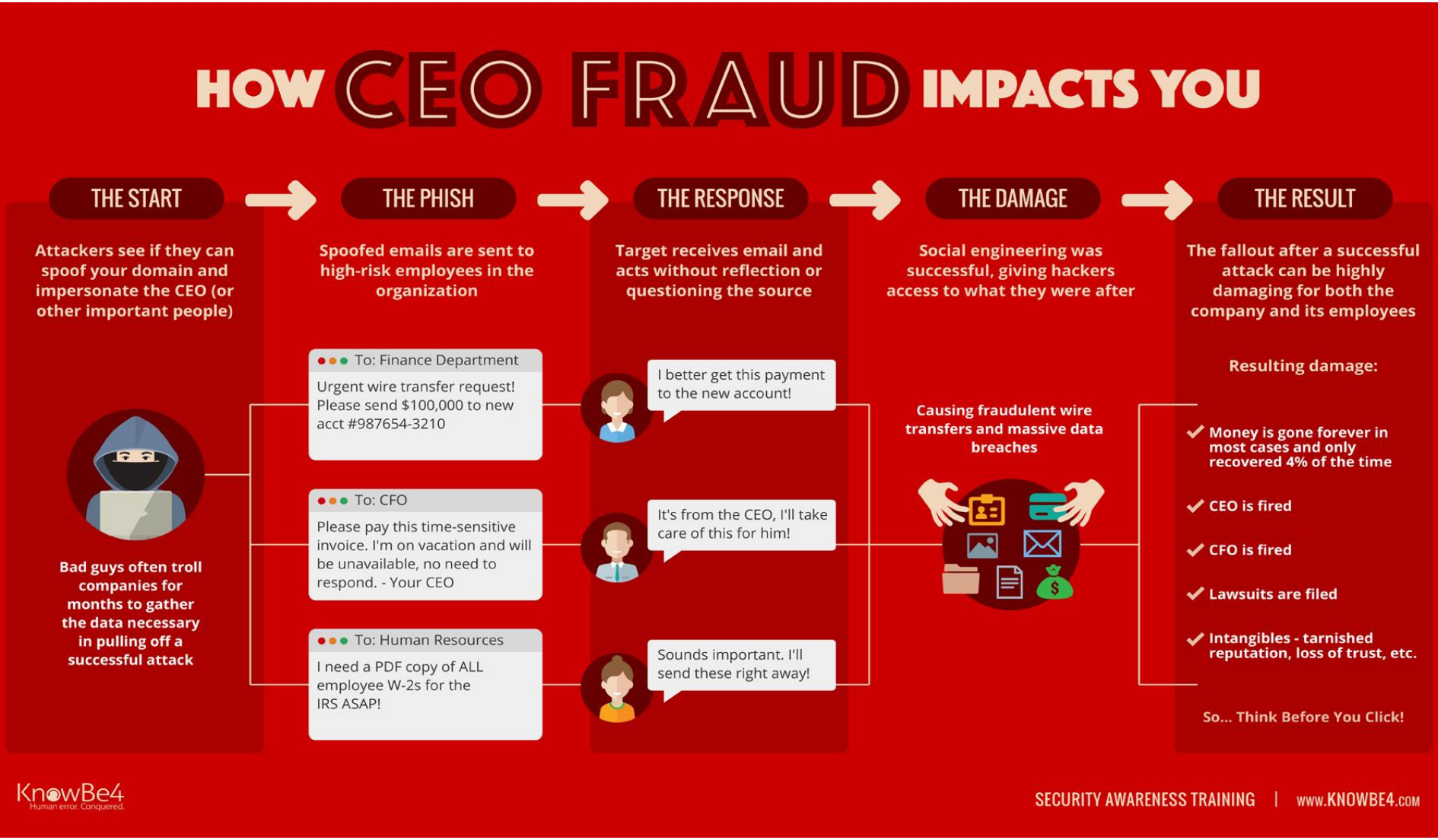


Figure 8.

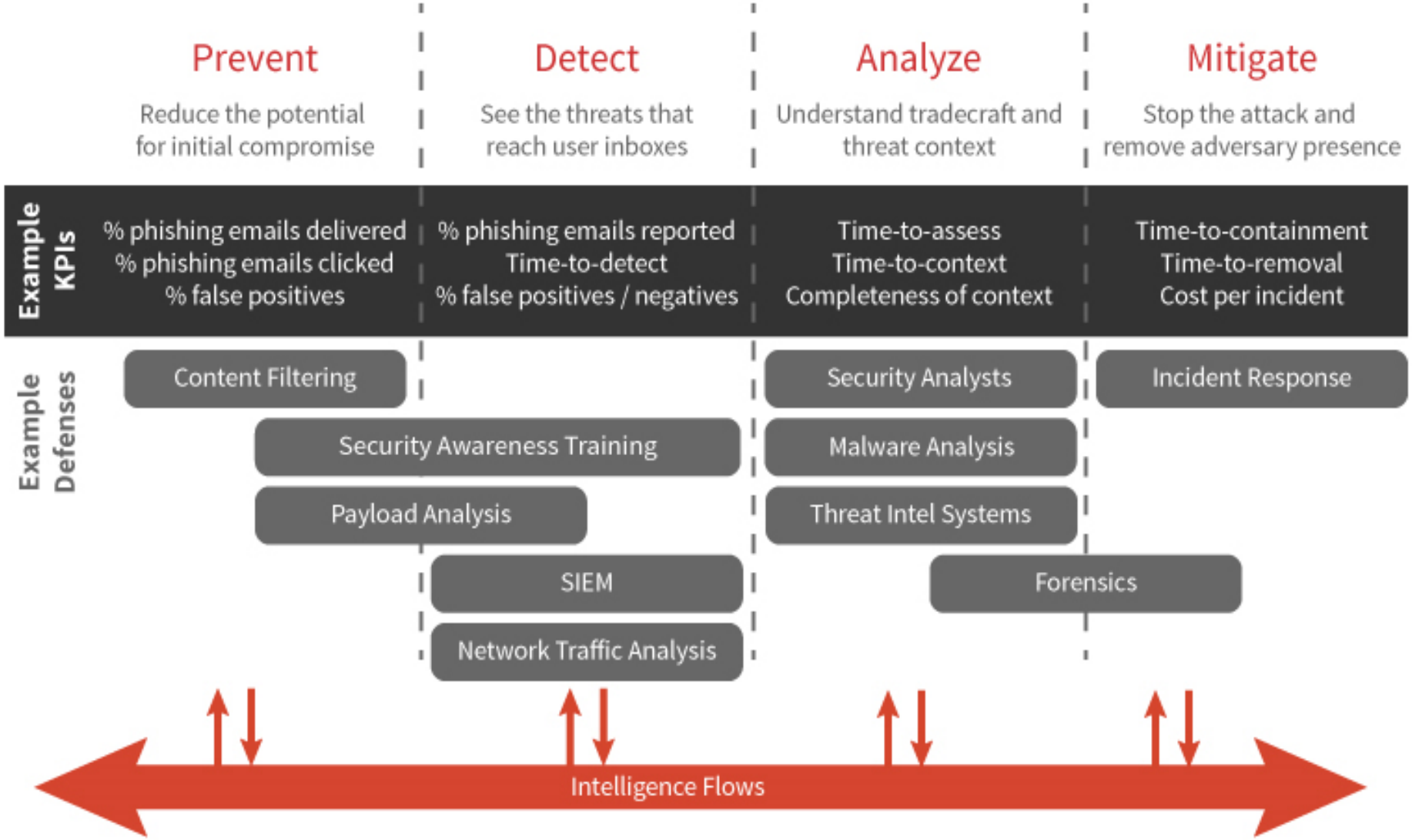
Percent of breaches where time to compromise (green)/time to discovery (blue) was days or less

Incremento dello spear phishing



The Defensive Framework for Spear Phishing

A strategic, end-to-end model for managing and improving protection against spear phishing attacks



deepcyber.it

ENISA fornisce un framework per la tassonomia completa delle minacce

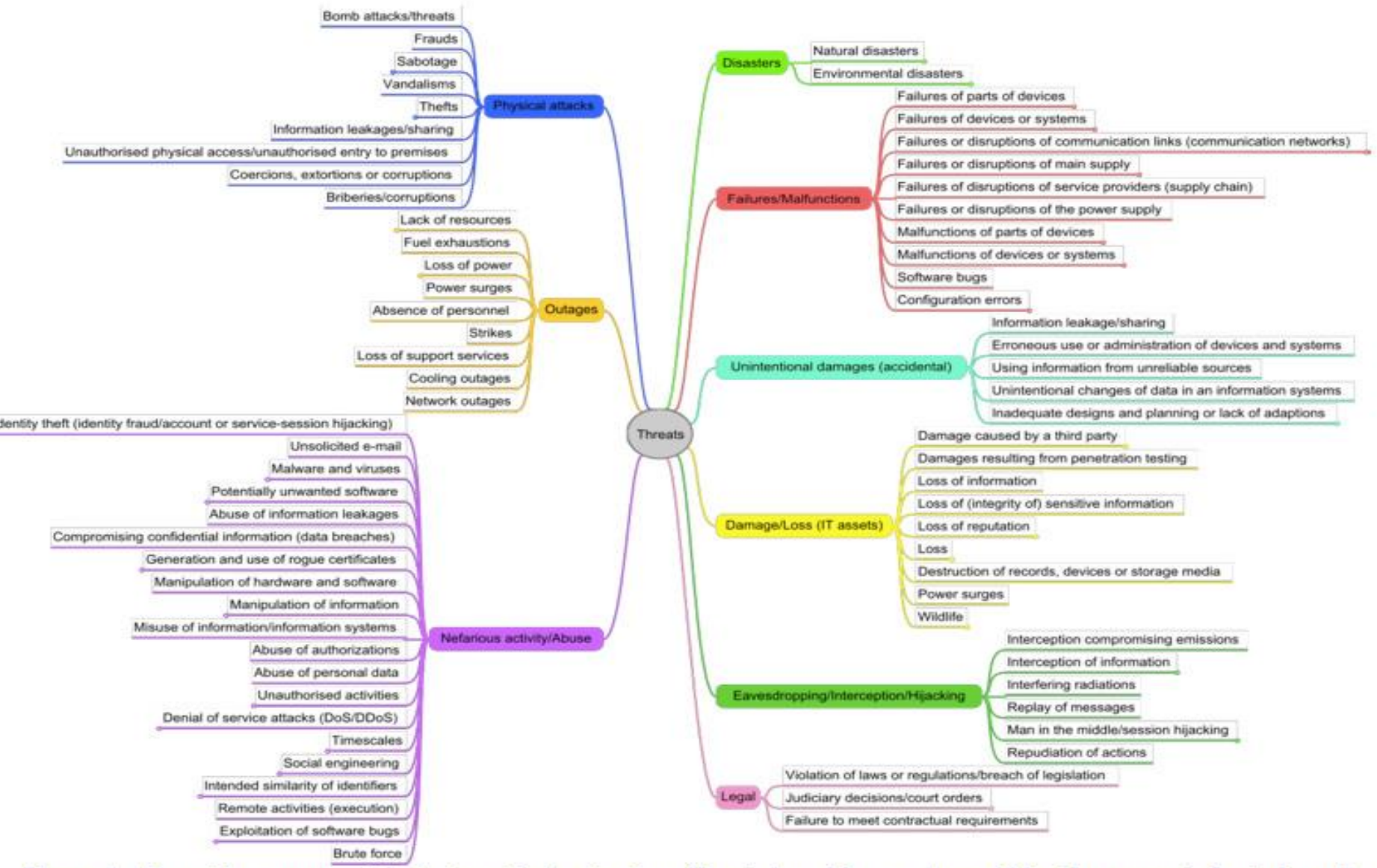


Figure 4 – Threat taxonomy of the Internet infrastructure (levels 1 and 2 - see Annex C for the expanded mind map)

La c.d. «minaccia cyber»

Insieme di condotte che possono essere realizzate nel e tramite il cyberspace

A differenza delle minacce tradizionali, quelle informatiche presentano CARATTERISTICHE PECULIARI, che ne rendono ardua l'azione repressiva:

- ✓ Compressione spazio-temporale
- ✓ Trasversalità
- ✓ Asimmetricità
- ✓ A-territorialità
- ✓ Continua mutevolezza

E' importante implementare delle contromisure ad hoc, fluide, come fluido è l'evolversi del mondo digitale, e che s'indirizzino non solo sul piano tecnologico, ma anche sul piano normativo e sociale.

Occorre un adeguato piano di CYBERSECURITY.

Altre problematiche...

- ✓ **Diversi** gli attori coinvolti, diversi gli interessi perseguiti (sicurezza nazionale, investigazione, aziende) e **diverso mindset**.

- ✓ Occorre un **approccio multidisciplinare** al tema. Le competenze sono diverse, e diverse le vulnerabilità a cui bisogna far fronte (tecniche, organizzative, delle persone).

DEEPCYBER

Agire ex ante o in modo «proattivo»...

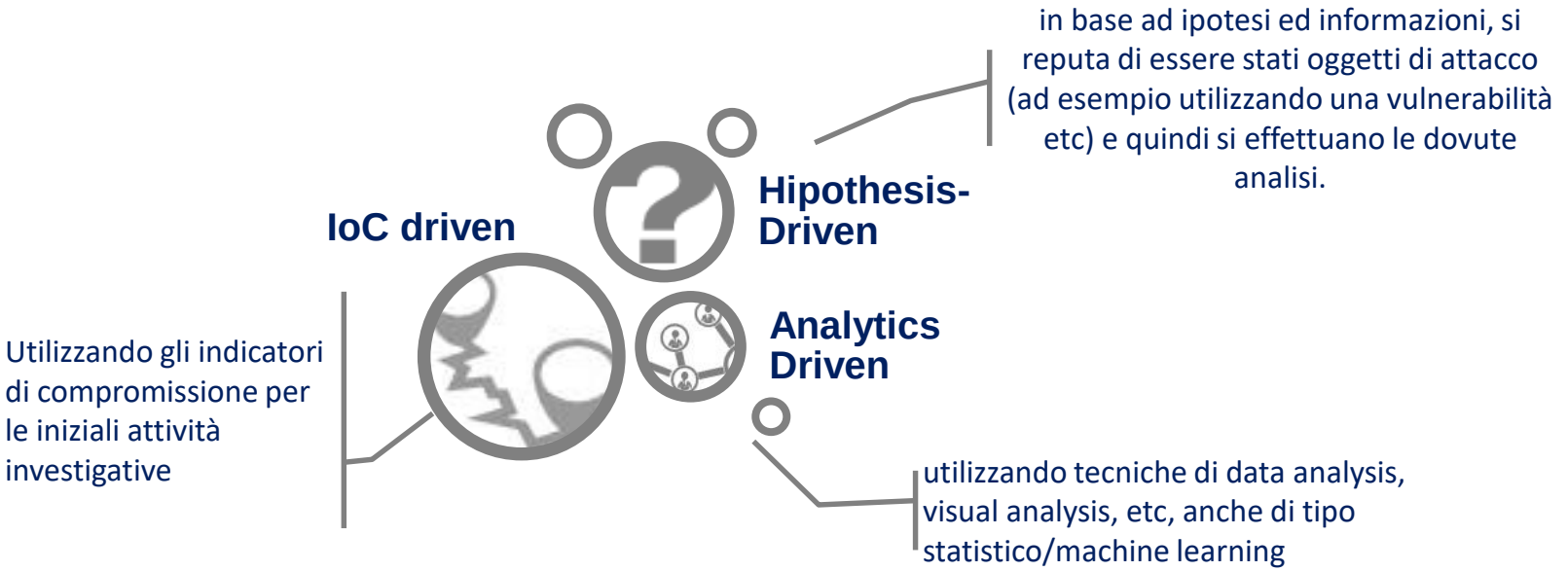
- ✓ **Cyber risk management:** Implementazione di un sistema di Information/Cyber Risk Management (anche in ambito ERM e sulla base del framework CIS-Sapienza e del NIST)

- ✓ **Security "by design"**: una Cybersecurity progettata all'inizio e non interpretata come un accessorio finale, integrata in tutto il ciclo di vita del sistema;

- ✓ **Cyber threat Intelligence:** per ridurre i tempi tra incidente e rilevazione dello stesso, si rende necessario attivare processi di raccolta informazioni esterne a supporto del knowledge interno. (anche, ma non solo, con Information sharing di settore e Partnership Pubblico Privato)

Tipici approcci per il cyber threat hunting

Esistono 3 tipologie di approccio relative al «cyber threat hunting» (source: Gartner nov 2015)



Solitamente, si riscontrano più di uno degli approcci sopra indicati

I feed della cyber threat intelligence

Fraud Analysis & AML
Leaked Corporate Accounts
Compromised Customer Accounts
Compromised Bank Cards
Money Mule Information
Compromised IMEI
AML Information

Social Networks
Social Networks Profiles
Search for People or Groups
Email Address Search & Correlation

Network Infrastructure
ICS-SCADA Vulns
Compromised SSL Certificate
Compromised or Infected Host
Data Heatmap
IP Addresses History
Geolocation Info

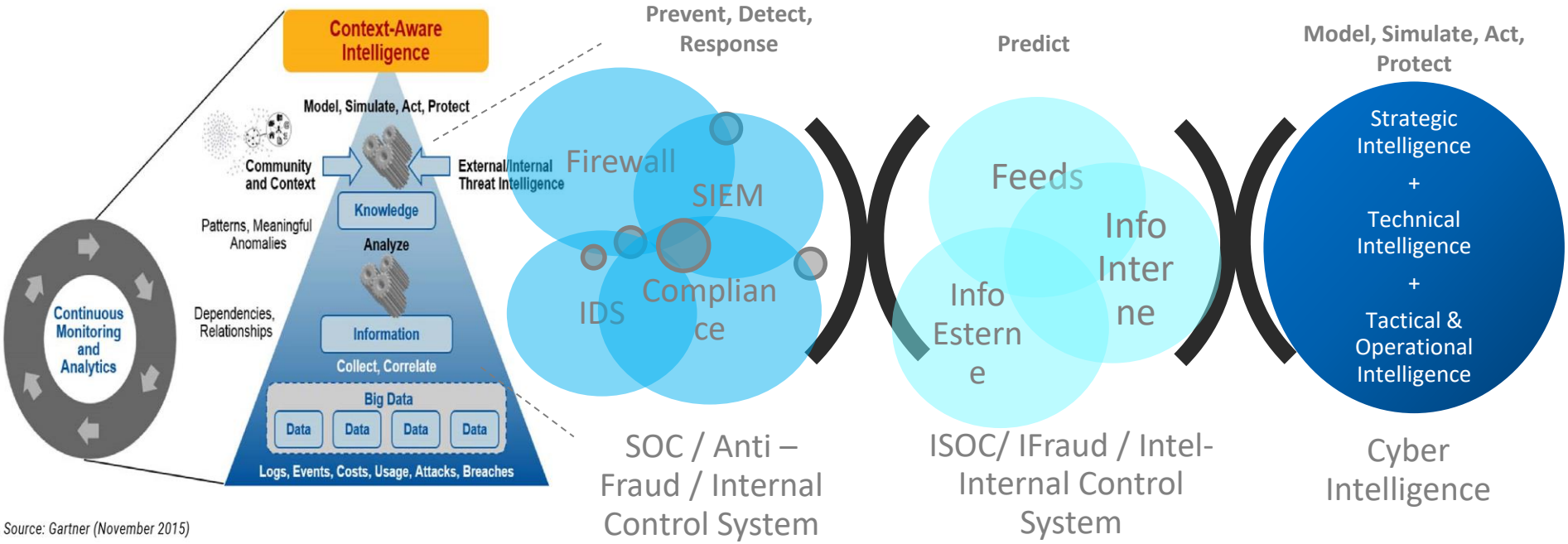
Physical Security
Critical Infrastructure
Geo-political conflict
ATM Infrastructure
IoT Threat & Weakness

SYSTEM & MOBILE MALWARE
CVE - Zero Day
Malware Details
Suspicius IP Addresses
Malware Components
Hashes' Payload
Exploited Vulnerability

BRAND REPUTATION
Domain Info & Reputation
Brand Reputation
Counterfeitting
Digital Piracy
Site Forgery
Cybersquatting

BAD ACTORS
Bad Actors Attributes
Attack's Target
Adversary Tactics, Tools & Procedures
Espionage Campaign

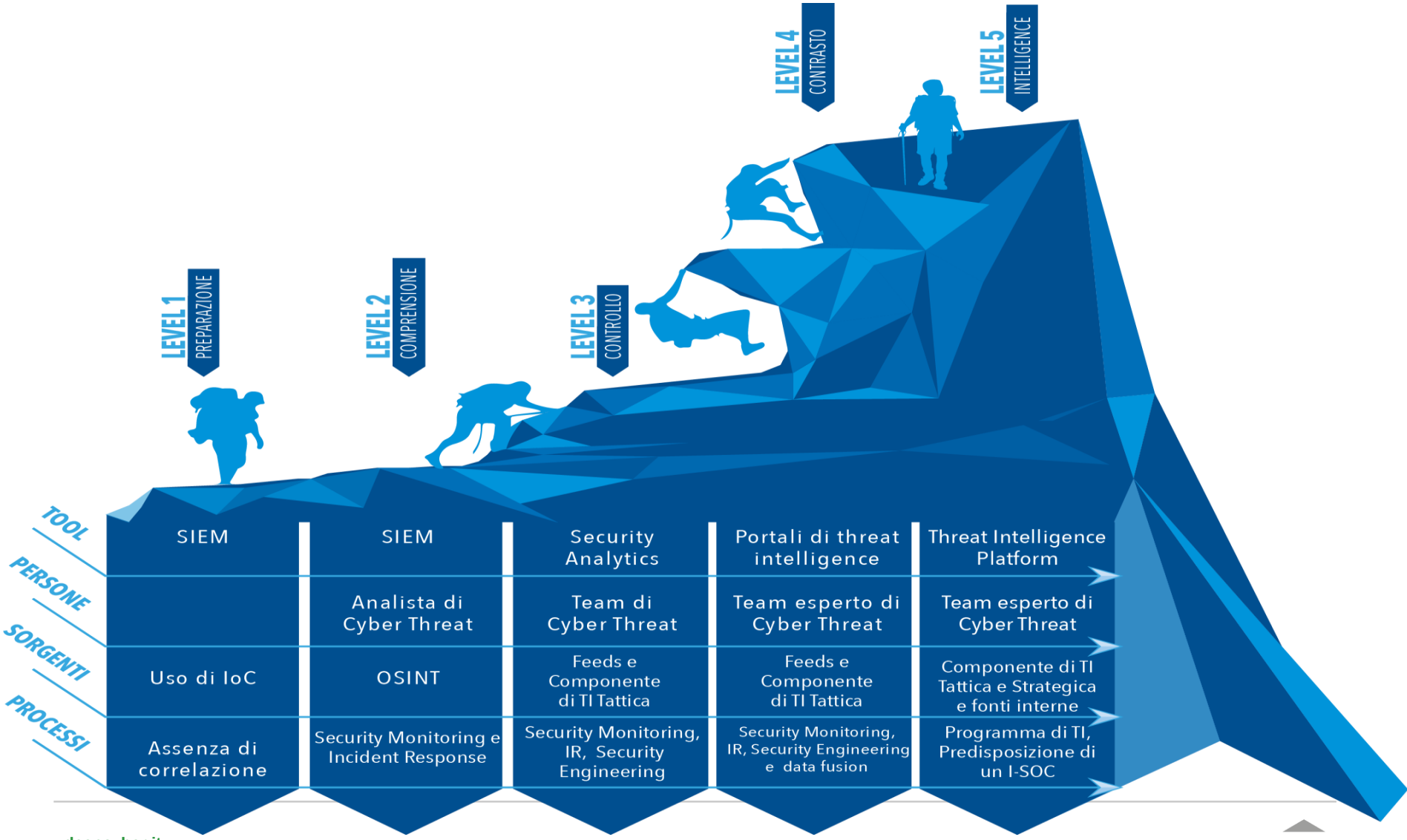
Intelligence driven «threat hunting»



Source: Gartner (November 2015)

I sistemi tradizionali come ***SOC, AML, Anti-Fraud & Internal Control system*** devono evolversi verso un modello "***Intelligence-Driven"***, in cui si utilizzano fonti diversificate, esterne ed interne (Logs, IoC, Attaccanti, Eventi AML) per rendere più proattiva l'attività di threat hunting, riducendo i tempi tra violazione/attacco e detection.

DeepCyber threat intelligence maturity model



Il linguaggio STIX / TAXII


NEW THREATS EVOLVE, READY TO GO DEEP